

LAW OFFICES
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC

2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213
TELEPHONE (202) 293-7060
FACSIMILE (202) 293-7860
www.sughrue.com

JC841 U.S. PTO
09/680258
10/05/00

October 5, 2000

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Junichi KOKUDO
AUTHENTICATION METHOD AND APPARATUS
AT WIRELESS LAN SYSTEM
Our Ref. Q61120

Dear Sir:

Attached hereto is the application identified above including 19 sheets of the specification, claims, 6 sheets of formal drawings, executed Assignment and PTO 1595 form, and executed Declaration and Power of Attorney.

The Government filing fee is calculated as follows:

Total claims	<u>11</u>	-	20	=	<u> </u>	x	\$18.00	=	<u> </u>	\$.00
Independent claims	<u>2</u>	-	3	=	<u> </u>	x	\$80.00	=	<u> </u>	\$.00
Base Fee										\$710.00
TOTAL FILING FEE										\$710.00
Recordation of Assignment										\$40.00
TOTAL FEE										\$750.00

Checks for the statutory filing fee of \$710.00 and Assignment recordation fee of \$40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from October 5, 1999 based on Japanese Application No. 284231/1999. The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: J. Frank Osha
J. Frank Osha
Registration No. 24,625

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

J. Kokudo
Filed 10/4/00
Q61120
10/1

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

1999年10月 5日

出 願 番 号
Application Number:

平成11年特許願第284231号

出 願 人
Applicant (s):

日本電気株式会社

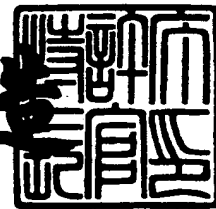
JC841 U.S. PTO
09/680258
10/05/00

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 7月14日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3054456

【書類名】 特許願

【整理番号】 49230041

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/28
H04B 7/26
H04Q 7/04

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 國土 順一

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100082935

【弁理士】

【氏名又は名称】 京本 直樹

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100082924

【弁理士】

【氏名又は名称】 福田 修一

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100085268

【弁理士】

【氏名又は名称】 河合 信明

【電話番号】 03-3454-1111

【手数料の表示】

【予納台帳番号】 008279

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9115699

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線 LAN システムにおける認証方法と認証装置

【特許請求の範囲】

【請求項 1】 無線 LAN システムにおける認証方法において、
端末局（STA）は帰属しようとするアクセスポイント（AP）に対して認証
要求し、

前記 AP は認証サーバに対して前記認証サーバに適合するプロトコルに変換し
て認証要求し、

前記認証サーバは前記 STA の MAC アドレスに基づき認証し、

前記 AP は前記 STA と所定の暗号化アルゴリズムに基づき暗号化認証を行な
うことを特徴とする無線 LAN システムにおける認証方法。

【請求項 2】 前記暗号化認証が正常に完了した後、前記認証サーバからの
指示により前記 AP の MAC アドレスのテーブルを更新することを特徴とする請
求項 1 記載の無線 LAN システムにおける認証方法。

【請求項 3】 前記認証サーバに障害が発生した場合に、前記 AP 単独にて
前記 MAC アドレスの認証を行なうことを特徴とする請求項 1 記載の無線 LAN
システムにおける認証方法。

【請求項 4】 前記暗号化アルゴリズムは、予め定められた使用期限を有す
る共通鍵に基づき暗号化されていることを特徴とする請求項 1 記載の無線 LAN
システムにおける認証方法。

【請求項 5】 前記共通鍵の期限が切れた場合に、オープンシステム認証方
式により MAC アドレス認証することを特徴とする請求項 4 記載の無線 LAN シ
ステムにおける認証方法。

【請求項 6】 前記オープンシステム認証方式の場合は、アソシエーション
した後、通信を行なう期間に所定の短時間の制限を設け、前記制限された時間内
に鍵配送することを特徴とする請求項 5 記載の無線 LAN システムにおける認証
方法。

【請求項 7】 無線 LAN システムにおける認証装置において、
端末局（STA）と所定の暗号化アルゴリズムに基づき認証すると共に認証サ

サーバと接続し、認証に関わる信号を前記認証サーバに適合するプロトコルに変換するアクセスポイント（ＡＰ）と、

前記変換された認証要求を受けて前記ＳＴＡのＭＡＣアドレスに基づき認証する前記認証サーバと

を有することを特徴とする無線ＬＡＮシステムにおける認証装置。

【請求項 8】 前記ＡＰは、前記暗号化認証が正常に完了した後、前記認証サーバからの指示により前記ＡＰのＭＡＣアドレスのテーブルを更新する手段を有することを特徴とする請求項 7 記載の無線ＬＡＮシステムにおける認証装置。

【請求項 9】 前記ＡＰは、前記認証サーバが故障した場合に、単独で前記ＭＡＣアドレスの認証を行うことを特徴とする請求項 7 記載の無線ＬＡＮシステムにおける認証装置。

【請求項 10】 前記所定の暗号化アルゴリズムは、ＩＥＥＥ 802.11 に規定されたＷＥＰアルゴリズムであることを特徴とする請求項 7 記載の無線ＬＡＮシステムにおける認証装置。

【請求項 11】 前記暗号化アルゴリズムは、使用期限を有する共通鍵を用いることを特徴とする請求項 7 記載の無線ＬＡＮシステムにおける認証装置。

【請求項 12】 前記共通鍵の期限が切れた場合に、オープンシステム認証方式によりＭＡＣアドレス認証することを特徴とする請求項 11 記載の無線ＬＡＮシステムにおける認証装置。

【請求項 13】 前記オープンシステム認証方式の場合は、アソシエーション後に、通信を行なう時間に所定の短時間の制限を設け、前記制限された時間内に鍵を配送することを特徴とする請求項 12 記載の無線ＬＡＮシステムにおける認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は無線ＬＡＮシステムの認証方法において、特にＩＥＥＥ 802.11（米国電気電子技術者協会が規定した国際標準）に準拠した無線ＬＡＮシステムの認証方法と認証装置に関する。

【0 0 0 2】

【従来の技術】

IEEE 802. 11 に準拠した無線 LAN システムは、今後普及が見込まれており免許不要で利用できる周波数帯（2. 4 GHz や 5 GHz）を使用できることから、無線区間のセキュリティ確保が重要になっている。

【0 0 0 3】

IEEE 802. 11 の第 8 章認証と暗号（8. AUTHENTICATION AND PRIVACY）には、オープンシステムを用いた認証方式（OPEN SYSTEM AUTHENTICATION）と WEP（WIRED EQUIVALENT PRIVACY）アルゴリズムを用いた共通（秘密）鍵認証方式（SHARED KEY AUTHENTICATION）とが規定されており、認証方式としてオープンシステム認証方式と共通鍵認証方式の 2 種類のどちらかが固定的に使用される。

【0 0 0 4】

図 5 は、IEEE 802. 11 に規定された無線 LAN システムの暗号化認証に関わる部分のブロック図を示す。

【0 0 0 5】

本図において、STA (STATION) 1 は、複数の端末局であり、各端末局は無線信号の送受信機能を有するノート PC 等のデータ端末である。

【0 0 0 6】

AP（アクセスポイント；ACCESS POINT）2 は、無線アクセスと有線網とのインターフェース機能や無線信号の送受信機能を有し、さらに無線信号制御等のファームウェアや MAC アドレス認証機能も搭載されている。

【0 0 0 7】

保守サーバ 4 は、AP 2 を SNMP で設定、管理を行なうサーバである。

【0 0 0 8】

STA 1 と AP 2 間の接続は無線区間 5 となっており、AP 2 と保守サーバ 4 間の接続はイーサネット等の有線区間が用いられている。

【0 0 0 9】

最初に、共通鍵認証方式について図を用いて説明する。

【0010】

図6は、IEEE 802.11で規定されたWEPアルゴリズムを用いた暗号化認証手順を示したシーケンス図である。本図において、WEPアルゴリズムによる暗号化認証はOSI (OPEN SYSTEM INTERCONNECT ION) の第2層のデータリンク層の副層であるMAC (媒体アクセス制御; MEDIA ACCESS CONTROL) において行われている。

【0011】

なお、MACは、複数の装置からのデータ送信要求が共通の伝送路上で競合したときのアクセス権制御や、装置と伝送路の物理的接続点の識別、フレーム形成、伝送路上の誤り制御などを第1層の物理層 (PHY; PHYSICAL LAYER) と一体化して行なう。

【0012】

あるSTA1からAP2に対して認証要求が無線信号にて送信される (S1)。このとき、PDUフォーマット内には共通鍵による認証要求であることを示すビットが用意されている。また、MACフレーム内にはソースアドレスとしてSTA1のMACアドレスが含まれている。

【0013】

認証要求を受けたAP2からSTA1に対してチャレンジテキストが送出される (S2)。チャレンジテキストを受けたSTA1は、WEPアルゴリズムに基づいて自分の共通鍵とIV (イニシャライゼイション ベクター; INITIALIZATION VECTOR) により暗号化する (S3)。

【0014】

次に、STA1は、暗号文とIVをAP2に対して送信する (S4)。AP2は、受信した暗号文とIVと自分の共通鍵により暗号文を復号化し、S2で送信したチャレンジテキストとS4で得られたチャレンジテキストとを比較して一致/不一致を判定する (S5)。

【0015】

AP2は、S4の判定結果が一致していた場合には、全体の認証が完了したと

して認証完了通知として SUCCESSFUL CODE を STA1 に送信する (S6)。認証完了通知を受けた AP1 は STA2 とアソシエーション (ASSOCIATION) の動作に移行する (S7)。

【0016】

一方、オープンシステム認証方式は、STA1 から AP2 に認証要求を送出すると、特段の確認手順を持たずに、AP2 から STA1 に対して認証結果が送出されるという簡単な手順である。

【0017】

【発明が解決しようとする課題】

以上説明した IEEE 802.11 の規定に準拠した無線 LAN システムにおける認証方法及び認証装置では、以下のような課題がある。

【0018】

第1に、前述した無線 LAN システムでは AP2 が MAC アドレスを認証している。しかし、一般に AP2 は無線アクセスと有線アクセスとのインターフェース機能をメインタスクとしているため、MAC アドレス認証機能のためのハードウェアやソフトウェアには制限がある。特に、通常用いられる AP2 では、多数の STA1 (例えば、10,000 台以上の STA1) の MAC アドレステーブルを用意するのは難しいため、多数の STA1 に対して MAC アドレス認証をすることが困難であった。

【0019】

第2に、最近は無線 LAN システムの端末局に無線信号を制御するためのファームウェアや ID 等が記憶されたカードが用いられるようになってきている。このような無線 LAN システムに IEEE 802.11 で規定された共通鍵認証方式を適用するためこのカードに鍵を記憶した場合には、カードは小型で持ち運び容易で、置き忘れや盗難し易く不正使用される確率が大いいため安全性を高める手段が必要となっていた。

【0020】

第3の課題は、オープンシステム認証方式では認証処理を完了し、アソシエー

ション後の通信期間に制限が無かったので、不正接続される可能性があり安全性が低かった。

【0 0 2 1】

以上説明したように本発明の目的は、これらの問題を解決した無線LANシステムの認証方法および認証装置を提供することにある。

【0 0 2 2】

【課題を解決するための手段】

本発明は上述した課題を解決するため、無線LANシステムにおける認証方法において、端末局（STA）は帰属しようとするアクセスポイント（AP）に対して認証要求し、

前記APは認証サーバに対して前記認証サーバに適合するプロトコルに変換して認証要求し、前記認証サーバは前記STAのMACアドレスに基づき認証し、前記APにチャレンジテキストを送出し、前記APは前記STAと所定の暗号化アルゴリズムに基づき暗号化認証を行なうことを特徴とする。

【0 0 2 3】

また、前記暗号化認証が正常に完了した後、前記認証サーバからの指示により前記APのMACアドレスのテーブルを更新することを特徴とする。

【0 0 2 4】

さらに、前記認証サーバに障害が発生した場合に、前記AP単独にて前記MACアドレスの認証を行なうことを特徴とする。

【0 0 2 5】

なお、前記暗号化アルゴリズムは、予め定められた使用期限を有する共通鍵に基づき暗号化されていることを特徴とする。

【0 0 2 6】

【発明の実施の形態】

本発明の無線LANシステムの認証方法と認証装置に関する実施の形態を図面を参照して説明する。

【0 0 2 7】

（第1の実施の形態）

本発明の実施の形態の無線LANシステムのシステム構成を示すブロック図を図1に示す。

【0028】

本図において、STA(STATION)1は、複数の端末局であり、各端末局はノートPC等のデータ端末10とデータ端末10に挿入されて無線信号の送受信や無線信号等の制御を行うハードウェアやファームウェアとが搭載された無線LANカード20とから構成される。

【0029】

AP(ACCESS POINT)2は、無線アクセスと有線網とのインターフェース機能を有し、また、無線信号の送受信や無線信号等の制御を行うハードウェアやファームウェアが搭載されている。また、IEEE802.11の認証プロトコル機能やSTA1との認証プロトコルを認証サーバの認証プロトコルに適合するようにプロトコル変換を行う機能を有する。

【0030】

認証サーバ3は、認証機能を有するサーバであり、使用可能なSTA1のMACアドレスは事前に登録されているものとする。本実施の形態では、ダイヤルアップ用アクセス、認証、課金等の機能を有するRADIUSサーバを用いて説明するが、これに限るものではない。また、AP2と接続してMACアドレス認証を行う機能を有する。

【0031】

また、保守サーバ4は、AP2をSNMPで設定、管理を行うサーバである。

【0032】

なお、本実施の形態では認証サーバ3と保守サーバ4とを独立した構成で示しているが、同一のサーバにこれら機能を搭載することもできる。

【0033】

ここで、STA1とAP2との接続は無線区間5で、AP2、認証サーバ3、保守サーバ4との接続はイーサネットケーブル等の有線区間6で行われている。

【0034】

図2は、本発明の無線LANシステムのコントロールプレーンの各ノードにお

けるプロトコルスタックを示す図である。

【 0 0 3 5 】

本図において、IEEE 802. 11では、帰属、認証はMAC副層の中のエンティティとして扱われる。無線区間5では、IEEE 802. 11に基づき暗号化認証が行われる。また、AP 2では、無線区間5の認証手順を受けると認証サーバ3まで認証要求を転送する。認証サーバ3は、RADIUSプロトコルを用いて認証処理を行なう。

【 0 0 3 6 】

図3は、本発明の無線LANシステムの具体的な認証方法のシーケンス図である。本図は、IEEE 802. 11で規定されたWEPメカニズムを利用した共通鍵を用いた暗号化認証方式に加えて、MACアドレスによる認証を行なっている。

【 0 0 3 7 】

前提条件として、STA 1およびAP 2の鍵設定は予めされており、使用可能なSTA 1のMACアドレスは認証サーバ3に登録されているものとする。

【 0 0 3 8 】

図1で説明したように、本発明の無線LANシステムでは、STA 1には無線LANカード20を用いているため、カードを置き忘れたり、盗難等により不正使用者の手に渡る可能性がある。このため、共通鍵に加えてMACアドレスによる認証を組み合わせることで安全性を高めている。なお、本図において図6と同一手順であるものには同一の番号を用いて説明する。

【 0 0 3 9 】

STA 1が立ちあがったとき、AP 2に対して認証要求を送出する(S1)。このとき、PDUフォーマット内には共通鍵認証方式による認証要求であることを示すビットが用意されている。このときのMACフレーム内にはソースアドレスとしてSTA 1のMACアドレスが含まれている。

【 0 0 4 0 】

要求を受けたAP 2は、図で示した通常のWEPメカニズムでは、チャレンジ用のテキストを用意してSTA 1へ送るが、ここではAP 2から認証サーバ3に

対して、MACアドレスを認証のIDとして、認証サーバ3へ認証要求する（S8）。

【0041】

ここで、認証サーバ3はRADIUSサーバとして、IETFのRFC2138で定義されるRADIUS（REMOTE AUTHENTICATION DIAL IN USER SERVICE）プロトコルに基づいて動作する。

【0042】

また、MACアドレスは、認証用プロトコル（RADIUSプロトコル）上ではユーザー名やコーリングステーションID（CALLING-STATION-ID）等として定義されている。

【0043】

認証（RADIUS）サーバ3は、AP2から受けたMACアドレスを認証する（S9）。

【0044】

次に、MACアドレスが認証された場合には、IETFのRFC1994で定義されるCHAPプロトコル（PPP CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL）と同様な手順に基づいてチャレンジテキストがAP2に対して送信される（S10）。ここで、PPPとは、Point-to-Point PROTOCOLをいう。

【0045】

なお、CHAPプロトコルでは一方向性のハッシュ方式としてメッセージダイジェスト5（MESSAGE DIGEST 2；MD5）が定められているが、それとは異なる方式を用いたり、有線路の安全性が確保されているとする場合は、ダミープロトコルとして使用しても良い。

【0046】

認証サーバ3からチャレンジテキストを受信したAP2は本来のWEPメカニズムに戻ってSTA1に対するチャレンジテキストをSTA1へ送信する（S2）。

【0047】

なお、このチャレンジテキストは、図のチャレンジテキストと同一であっても良いし、認証サーバ3からのチャレンジテキストを流用しても良い。

【0048】

STA1はAP2より受信したチャレンジテキストに対し、WEPメカニズムにより自分の共通鍵とイニシャライゼーションベクタ (INITIALIZATION VECTOR; IV) により暗号化を行う (S3)。

【0049】

この暗号文とイニシャライゼーションベクタは、STA1からAP2へ送信される (S4)。

【0050】

AP2は、受信した暗号文とイニシャライゼーションベクタと自分の共通鍵により暗号文を復号し、元のチャレンジテキストに戻れば、無線区間の認証が成功したものとする (S5)。

【0051】

AP2は、認証サーバ3にCHAPによりハッシュを行ってCHAPレスポンスを返す (S11)。

【0052】

なお、CHAPをダミープロトコルとする場合は、CHAPレスポンス相当の返答に変えて返答する。

【0053】

認証サーバ3ではCHAPにより正常なレスポンスを受け取ったことが分かったと、全体の認証が完了したとして、AP2に対して認証完了の通知をする (S12)。

【0054】

認証完了通知を受けたAP2はSTA1に対して認証完了を通知し、STA1も認証が成功したことを認知する (S6)。

【0055】

また、認証サーバ3は、AP2に保存されている接続可能なMACアドレステーブルを更新するよう指示を行なう (S13)。この結果、新たに認証されたM

ACアドレスが随時更新登録されることになり、AP 2のMACアドレス管理テーブルの動的な更新を可能とする。

【 0 0 5 6 】

その後、STA 1とAP 2とは、アソシエーションの動作へ移る（S 7）。

【 0 0 5 7 】

（第 2 の実施の形態）

本発明の第 2 の実施の形態は、図 3 のシーケンスにおいて、認証サーバ 3 にハードやソフト等の障害が発生し、AP 2からの認証サーバ 3 に対する認証要求（S 8）が受け付けられない場合に、AP 2単体でMACアドレスによる認証を行うフローが追加されたことである。

【 0 0 5 8 】

これは、図 3 のシーケンスの（S 1 3）で説明したようにAP 2のMACアドレステーブルは動的に更新されているため、認証結果がAP 2のMACアドレステーブルに即時反映され、AP 2は障害直前までのMACアドレス情報を知っているためAP 2単体のMACアドレス認証ができる。この結果、たとえ認証サーバ 3 に障害等が発生しても認証手順を継続することができる。

【 0 0 5 9 】

（第 3 の実施の形態）

本発明の第 3 の実施の形態としては、共通鍵の使用時間に予め所定の期限を設けて安全性を高めるものである。

【 0 0 6 0 】

図 3 のシーケンスの（S 3）において、STA 1の自分の共通鍵を用いて常時暗号化できるようになっていたが、共通鍵が漏洩される等の場合においても不正認証が行われることのないよう本実施形態で一定の保護を設けることができる。

【 0 0 6 1 】

（第 4 の実施の形態）

前述した本発明の第 3 の実施の形態では、WEP用共通鍵に使用期限を設けることで不正使用者の保護は図れる。しかし、正規の使用者が本使用期限内にSTA 1を使用しなかった場合等では、使用期限以降に再度使用可能とするため鍵の

配送を行う必要がある。

【 0 0 6 2 】

本発明の第 4 の実施の形態はこのような共通鍵が使用期限により無効となった場合の認証方法に関するものである。

【 0 0 6 3 】

図 4 は、本発明の第 4 の実施の形態の認証手順を示すシーケンス図を示している。

【 0 0 6 4 】

本図において、STA 1 からの共通鍵認証が無効となった場合、STA 1 は AP 2 に対して再度オープンシステム認証方式により認証要求する (S 1 4) 。

【 0 0 6 5 】

要求された AP 2 は、オープンシステム認証方式であることを知り、AP 1 から認証サーバ 3 に対して、MAC アドレスを認証の ID として認証要求する (S 1 5) 。

【 0 0 6 6 】

ここで、認証サーバ 3 は、例えば、RADIUS サーバとして IETF の RFC 2 1 3 8 で定義される RADIUS プロトコルに基づいて動作する。

【 0 0 6 7 】

また、MAC アドレスは、認証用プロトコル (RADIUS) 上ではユーザー名やコーリングステーション ID (CALLING-STATION-ID) 等として定義されている。

【 0 0 6 8 】

次に、認証 (RADIUS) サーバ 3 は、MAC アドレスを認証した後、IETF の RFC 1 9 9 4 で定義される CHAP プロトコルと同様な手順に基づいてチャレンジテキストが AP 2 に対して送信される (S 1 6) 。

【 0 0 6 9 】

ここで、CHAP プロトコルでは一方向性のハッシュ方式として MD 5 が定められているが、それとは異なる方式を用いたり、有線路の安全性が確保されているとする場合は、ダミープロトコルとして使用しても良い。

【0070】

認証サーバ3からチャレンジテキストを受信したAP2は認証サーバ3に対しCHAPによりハッシュを行ってCHAPレスポンスを返す(S17)。

【0071】

なお、CHAPをダミープロトコルとする場合は、CHAPレスポンス相当の返答に変えて返答する。

【0072】

認証サーバ3は、CHAPにより正常なレスポンスを受け取ったことが分かったと、全体の認証が完了したとして、AP2に対して認証完了の通知をする(S18)。

【0073】

認証完了通知を受けたAP2はSTA1に対して認証完了通知し、STA1も認証が成功したことを認知する(S19)。

【0074】

その後、STA1とAP2とはアソシエーションの動作へ移る(S20)。

【0075】

なお、AP2と認証サーバ3間で認証に成功した場合、第1の実施の形態で説明したようにAP2に保存されている接続可能MACアドレステーブルに対して、新たに認証したMACアドレスを更新登録しても良いが、本実施の形態の場合にはオープンシステム認証方式なので安全性が低いためMACアドレスの更新登録を行わないのが望ましい。

【0076】

アソシエーション手順が完了すれば、STA1はAP2を通して通常のIPパケットによる通信を行なう(S21)。

【0077】

(第5の実施の形態)

第4の実施の形態におけるオープンシステム認証方式の場合に、アソシエーション後の通信期間に制限がなかったため、不正接続が行われる可能性が高い。

【0078】

本発明の第 5 の実施の形態では、アソシエーション後の通信期間の有効期間を、例えば、公開鍵配送方式などにより鍵管理サーバから W E P メカニズムの共通鍵を配送されるに十分な一定の短い時間に定める。この時間は、例えば、1 0 秒から 1 分程度が望ましい。

【 0 0 7 9 】

そして、図 4 において、本来の共通鍵認証のための鍵配送を受けた後、デアソシエーションし（S 2 2）、再度共通鍵認証方式で接続する。

この結果、MAC アドレスを偽る不正アクセスがあったとしても、セキュリティを向上する効果をもたらす。

【 0 0 8 0 】

【発明の効果】

以上説明したように、本願発明の無線 L A N システムの認証方法および認証装置は、以下の効果を有している。

【 0 0 8 1 】

第 1 に、I E E E 8 0 2 . 1 1 で規定された共通鍵認証方式を拡張して MAC アドレス認証を行なっている。このため、無線 L A N カードを用いるため不正使用等が起きやすい無線 L A N システムにおいても、高い安全性を確保することができる。また、非常に多数の無線 L A N カードに対する認証をいずれのアクセスポイントからでも行なえる効果も有している。

【 0 0 8 2 】

第 2 に、W E P の共通鍵に使用期限を設けたり、オープンシステム認証方式でアソシエーションされている期間を限定したりしてさらに、安全性を高めることができる。

【 0 0 8 3 】

第 3 に、A P における MAC アドレステーブルは認証サーバからの指示で動的に更新されているため、認証サーバが障害になっても、障害直前までの MAC アドレス情報を利用して A P 単独で MAC アドレス認証ができる。

なお、本発明が上記各実施の形態に限定されず、本発明の技術思想の範囲内において、各実施の形態は適宜変更され得ることは明らかである。

【図面の簡単な説明】

【図 1】

本発明の無線 LAN システムのシステム構成を示すブロック図である。

【図 2】

図 1 の各ノードのプロトコルスタックを示す図である。

【図 3】

図 1 の認証手順を示すシーケンス図である。

【図 4】

本発明の共通鍵が無効になった場合の認証手順を示すシーケンス図である。

【図 5】

IEEE 802. 11 に規定された無線 LAN システムの認証方法に関するシステム構成を示すブロック図である。

【図 6】

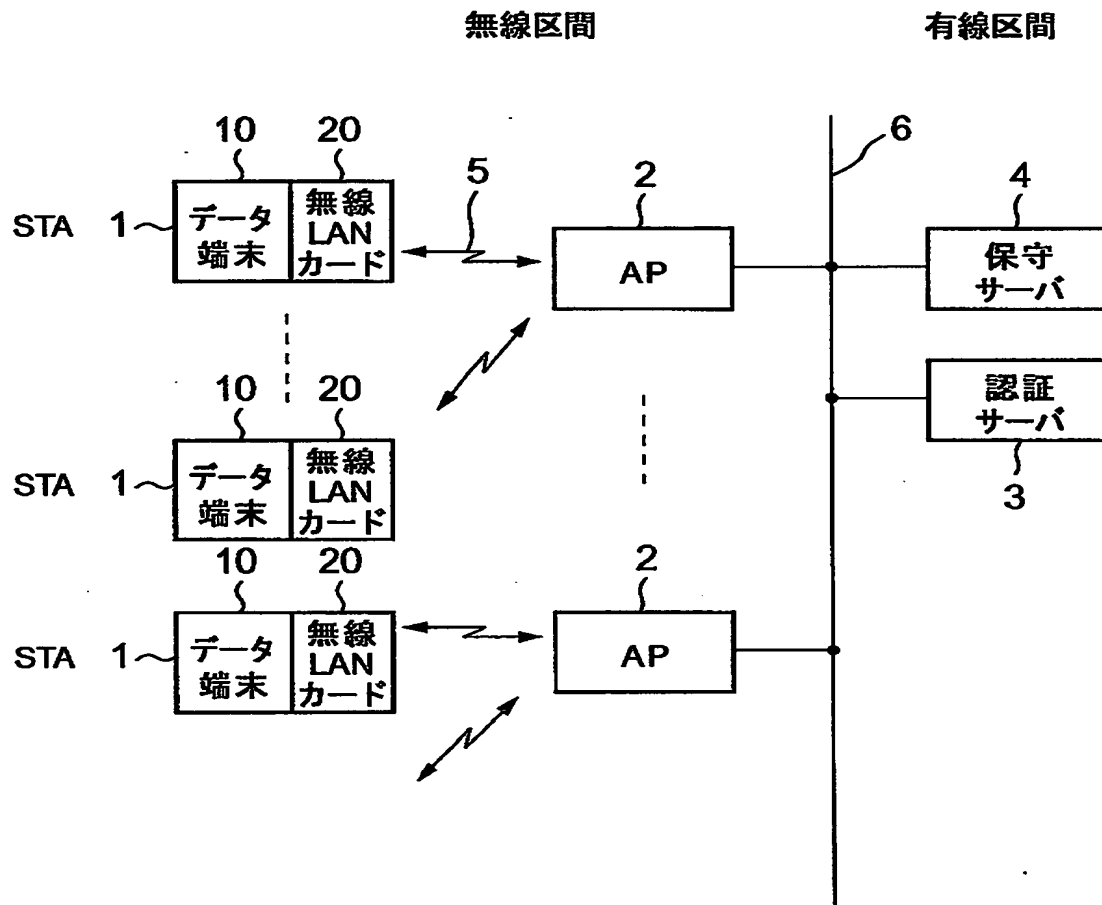
図 5 の認証手順を示すブロック図である。

【符号の説明】

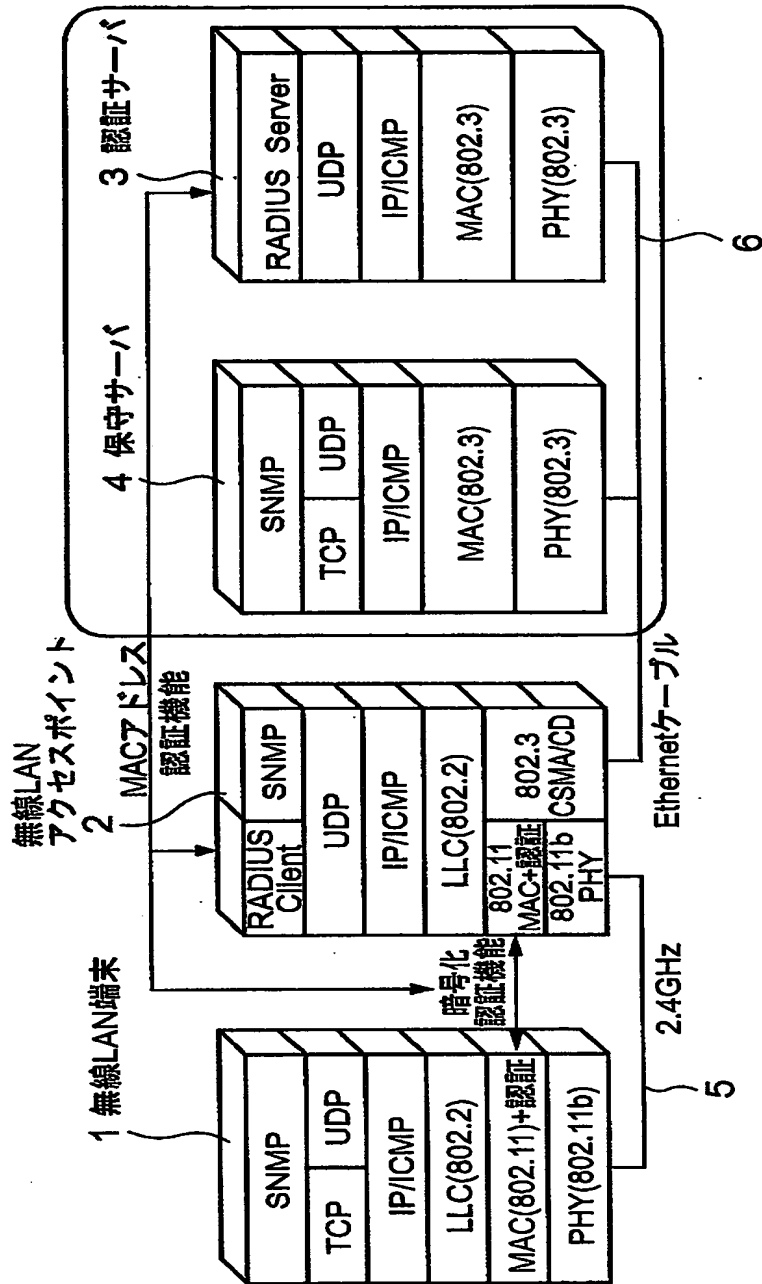
- | | |
|----|------------|
| 1 | STA |
| 2 | AP |
| 3 | 認証サーバ |
| 4 | 保守管理サーバ |
| 5 | 無線区間 |
| 6 | 有線区間 |
| 10 | ノート PC 等 |
| 20 | 無線 LAN カード |

【書類名】 図面

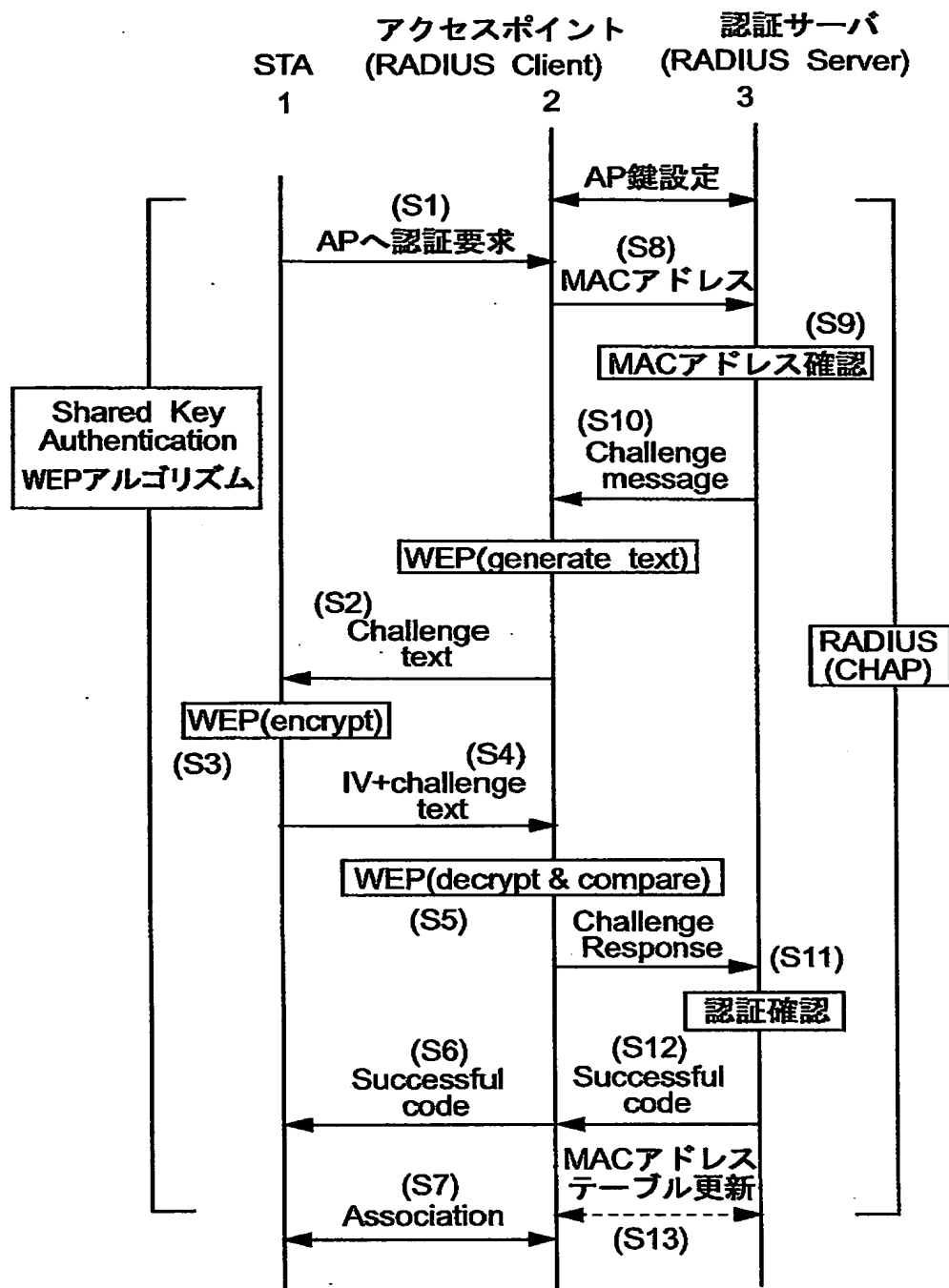
【図 1】



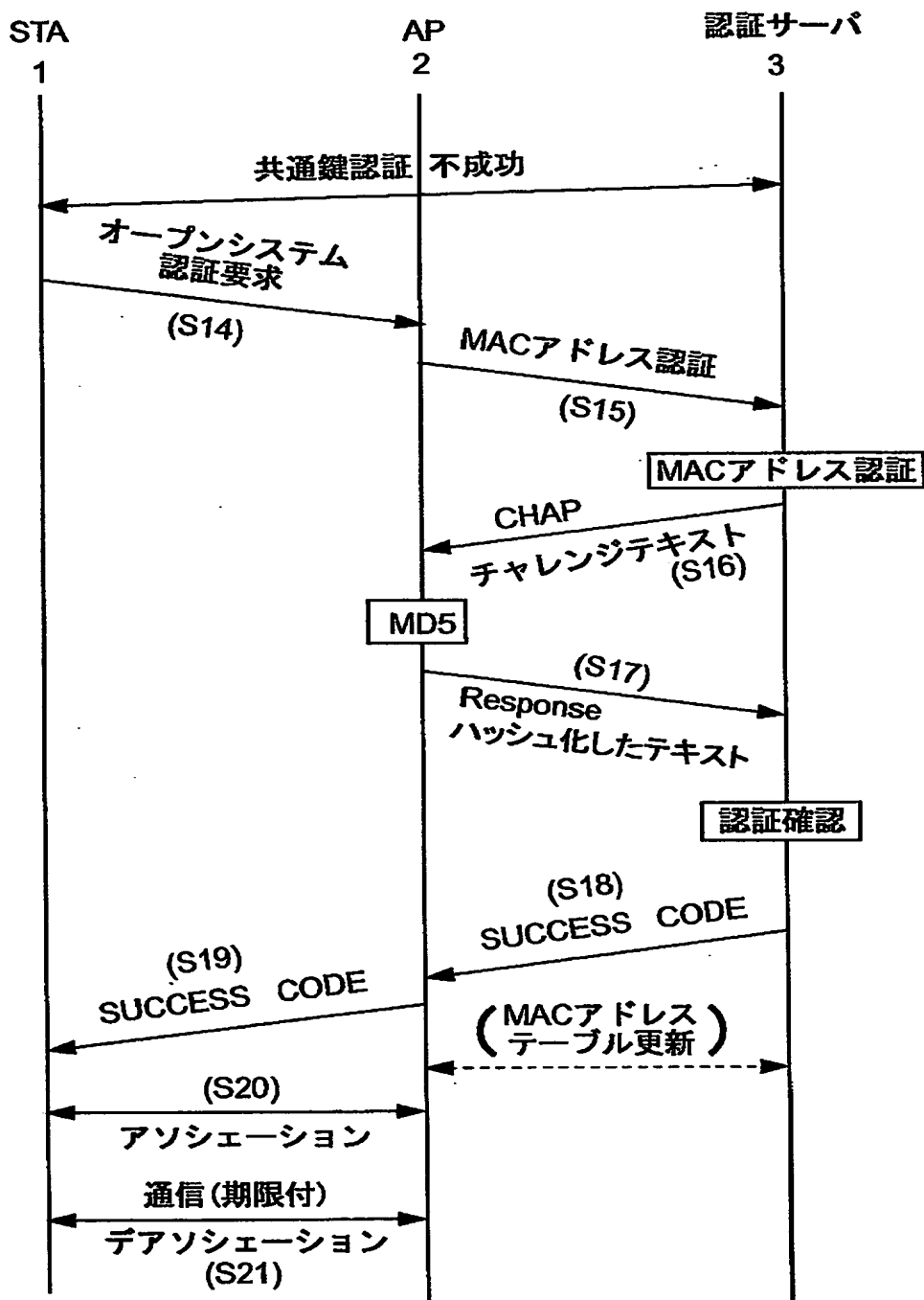
【図 2】



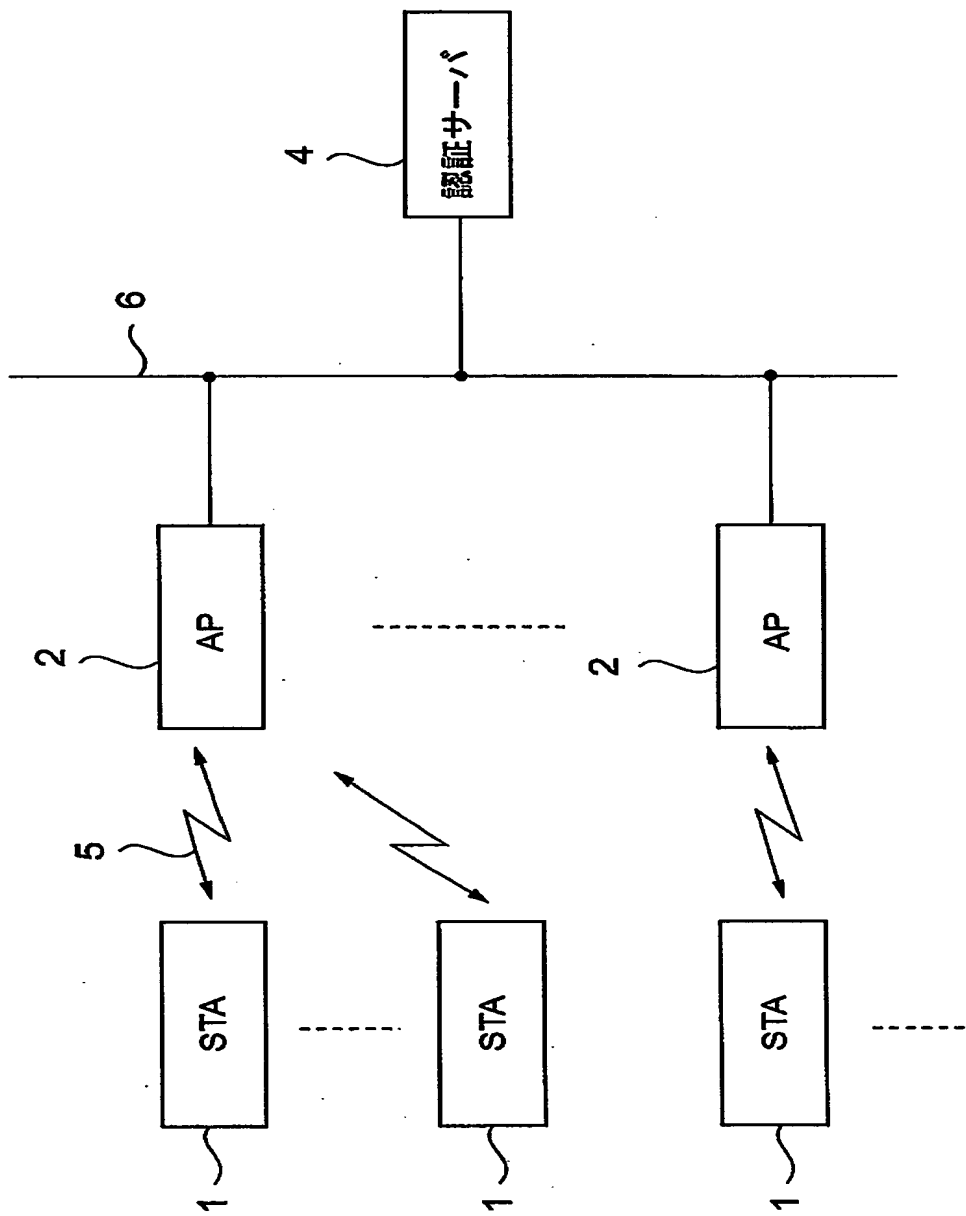
【図 3】



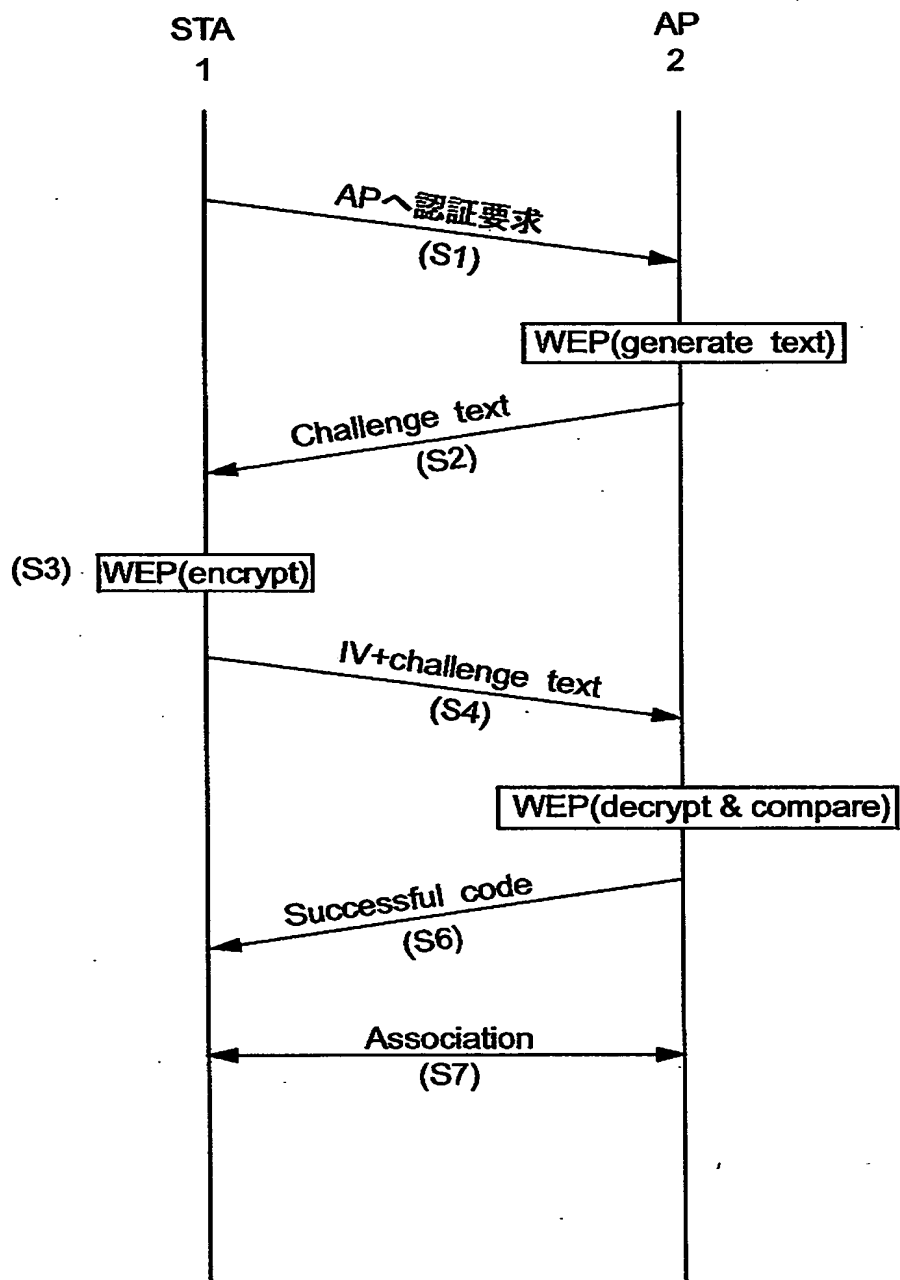
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 I E E E 8 0 2 . 1 1 に準拠した無線 L A N システムの暗号化認証方法と認証装置について、アクセスポイント (A P) に多数の加入者局 (S T A) を接続して安全に認証できる構成を提供する。

【解決手段】 データ端末 1 0 と無線 L A N カード 2 0 からなる多数の S T A 1 から A P 2 に対して認証要求を送出する (S 1) 。 A P 2 は認証サーバ (R A D I U S) サーバ 3 に対して、認証サーバ 3 のプロトコルで M A C アドレスを送出する (S 8) 。 認証サーバ 3 は、 M A C アドレス認証を実行した (S 9) 後、チャレンジテキストを A P 2 に送出的 (S 1 0) 。 A P 2 は、 1 E E E 8 0 2 . 1 1 で定められた W E P アルゴリズムの処理に従って、 S T A 1 と暗号化認証を行なう (S 2) ～ (S 6) 。

【選択図】 図 3

認定・付加情報

特許出願の番号	平成 1 1 年 特許願 第 2 8 4 2 3 1 号
受付番号	5 9 9 0 0 9 7 5 0 3 7
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 1 年 1 0 月 7 日

<認定情報・付加情報>

【提出日】	平成11年10月 5日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 2 3 7]

1. 変更年月日	1 9 9 0 年 8 月 2 9 日
[変更理由]	新規登録
住 所	東京都港区芝五丁目 7 番 1 号
氏 名	日本電気株式会社